Version Number: 01-2017

U.S. Department of Commerce
National Institute of Standards and Technology
(NIST)

Privacy Threshold Analysis
for the
Information Technology Laboratory (ITL) Research System
(770-01)

U.S. Department of Commerce Privacy Threshold Analysis
National Institute of Standards and Technology (NIST)

Unique Project Identifier: 770-01

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description of the information system in a way that a non-technical person can understand.*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C, § 3502(8).

a) Whether it is a general support system, major application, or other type of system

The Information Technology Laboratory (ITL) has the broad mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology through research and development in information technology, mathematics, and statistics. In support of this mission, NIST conducts research on various biometric modalities, engaging in national and international standards development, and testing and evaluating technology using biometrics, as follows:

The Biometric Research Data (BRD) project is comprised of large biometric data sets from which identifiable private information has been removed. The data sets are collected by non-NIST entities for their own research purposes, then released to NIST through partnering research agreements. NIST uses the data sets for its own biometric research (e.g., generation of metrics, etc.). In addition, after preparation by NIST, the data is made available to researchers from the public. Researchers must accept terms of usage and provide business contact information through a web registration application before they can access the data sets.

The Facial Forensic Comparison project is comprised of biometric data sets, specifically individual facial images, collected by non-NIST entities for their own research purposes, then released to NIST through a partnering research agreement. Identifiable private information has been removed from these data sets.

b) System location

The BRD components (i.e., host server(s), database(s), and application) supporting the BRD are located at the NIST Gaithersburg, Maryland, and Boulder, Colorado, facilities

within the continental United States, and/or Seattle, Washington. The Facial Forensic Comparison data sets are stored on a stand-alone storage system located at the NIST Gaithersburg, Maryland, facility within the continental United States.

c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*

The system does not share information. However, the data is made available to researchers who have accepted terms of usage.

d) *The purpose that the system is designed to serve*

The components support the research mission of NIST.

e) *The way the system operates to achieve the purpose*

- BRD: A researcher registers with their business contact information through a web application, which requires acceptance of terms of usage (e.g., research purposes). Following submission, a dynamic URL (expiring after 1 week) is returned to the requestor, allowing the requestor to download the biometric dataset (e.g., NIST Special Database 300), either in part or full.
- Facial Forensics Comparison: NIST Federal employees and contractors visually inspect facial images for perceptual accuracy through a custom developed application. Research results are documented.

f) *A general description of the type of information collected, maintained, use, or disseminated by the system*

In addition to work-related data and general purpose data, biometrics are collected, maintained, used, or disseminated by the system.

g) *Identify individuals who have access to information on the system*

- BRD: The public has access to download the data set after registration and acceptance of terms.
- Facial Forensics Comparison: Only authorized NIST staff and research participants have access to information on the system.

h) *How information in the system is retrieved by the user*

The information collection is new, and the public has access to download the data set after registration and acceptance of terms.

i) *How information is transmitted to and from the system*

See description in *e)*.

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

__X_ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access	X	h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): New data					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

__X_ Yes. *Please describe the activities which may raise privacy concerns.*
Biometric Research data sets.

____ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

____ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

____ Companies

____ Other business entities

__X_ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc.., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

__X_ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

____ DOC employees

____ Contractors working on behalf of DOC

__X_ Members of the public (research participants)

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

__X_ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

__X_ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the Information Technology Laboratory (ITL) Research System (770-01), and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the Information Technology Laboratory (ITL) Research System (770-01), and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO):

James St. Pierre

Signature of SO: _____ Date: May 24, 2019

Name of Information Technology Security Officer (ITSO):

K. Robert Glenn

Signature of ITSO: _____ Date: 5/29/19

Name of Co-Authorizing Official (AO):

Charles Romine

Signature of AO: _____ Date: 28 May 2019

Name of Co-Authorizing Official (AO)/Bureau Chief Privacy Officer (BCPO):

Susannah Schiller, Acting

Signature of AO/BCPO: _____ Date: 5/29/19